Cybersecurity in health – disentangling value tensions

Loi, Michele ; Christen, Markus ; Kleine, Nadine ; Weber, Karsten

Abstract: Purpose Cybersecurity in healthcare has become an urgent matter in recent years due to various malicious attacks on hospitals and other parts of the healthcare infrastructure. The purpose of this paper is to provide an outline of how core values of the health systems, such as the principles of biomedical ethics, are in a supportive or conflicting relation to cybersecurity. Design/methodology/approach This paper claims that it is possible to map the desiderata relevant to cybersecurity onto the four principles of medical ethics, i.e. beneficence, non-maleficence, autonomy and justice, and explore value conflicts in that way. Findings With respect to the question of how these principles should be balanced, there are reasons to think that the priority of autonomy relative to beneficence and non-maleficence in contemporary medical ethics could be extended to value conflicts in health-related cybersecurity. Research limitations/implications However, the tension between autonomy and justice, which relates to the desideratum of usability of information and communication technology systems, cannot be ignored even if one assumes that respect for autonomy should take priority over other moral concerns. Originality/value In terms of value conflicts, most discussions in healthcare deal with the conflict of balancing efficiency and privacy given the sensible nature of health information. In this paper, the authors provide a broader and more detailed outline.

DOI: https://doi.org/10.1108/jices-12-2018-0095

Cybersecurity in health – disentangling value tensions

Michele Loi and Markus Christen
Digital Society Initiative, University of Zurich, Zurich, Switzerland, and
Nadine Kleine and Karsten Weber
Institute for Social Research and Technology Assessment, Ostbayerische Technische Hochschule Regensburg, Regensburg, Germany

Received 3 December 2018
Revised 25 January 2019
Accepted 29 January 2019

Abstract

Purpose – Cybersecurity in healthcare has become an urgent matter in recent years due to various malicious attacks on hospitals and other parts of the healthcare infrastructure. The purpose of this paper is to provide an outline of how core values of the health systems, such as the principles of biomedical ethics, are in a supportive or conflicting relation to cybersecurity.

Design/methodology/approach – This paper claims that it is possible to map the desiderata relevant to cybersecurity onto the four principles of medical ethics, i.e. beneficence, non-maleficence, autonomy and justice, and explore value conflicts in that way.

Findings – With respect to the question of how these principles should be balanced, there are reasons to think that the priority of autonomy relative to beneficence and non-maleficence in contemporary medical ethics could be extended to value conflicts in health-related cybersecurity.

Research limitations/implications – However, the tension between autonomy and justice, which relates to the desideratum of usability of information and communication technology systems, cannot be ignored even if one assumes that respect for autonomy should take priority over other moral concerns.

Originality/value – In terms of value conflicts, most discussions in healthcare deal with the conflict of balancing efficiency and privacy given the sensible nature of health information. In this paper, the authors provide a broader and more detailed outline.

Keywords Ethics, Healthcare, Cybersecurity, Computer ethics, Bioethics, e-Health

Paper type Conceptual paper

1. Introduction

Recent global attacks such as the WannaCry ransomware attack in May 2017 had considerable effects on the information and communication technology (ICT) infrastructure of many healthcare providers, indicating that cybersecurity in healthcare is rather underdeveloped compared to other domains such as the financial sector (ENISA, 2016). What is the reason for this given that everybody agrees that health is an important value to human beings and that health information is among the most sensitive information? We suggest that one reason for this problem are the many values relevant for healthcare that are often in a conflicting tension with the aim of cybersecurity, as shown in Figure 1. Although one may claim that cybersecurity prevents damage from malicious attackers (i.e. supports

Journal of Information, Communication and Ethics in Society
Vol. 17 No. 2, 2019
pp. 229-245
Emerald Publishing Limited
1477-996X
DOI 10.1108/JICES-12-2018-0095

non-maleficence), enables the protection of privacy and in this way usually enables trust, both moral (such as equality or care) and instrumental values (such as cost-effectiveness or efficiency) can have a conflicting relation to cybersecurity. For example, cybersecurity measures are costly and often effortful.

As an illustration, take the example of autonomy. When ICT is used in healthcare, it shall be aimed at ensuring that patients themselves determine which information is revealed to whom. Generally, password protection and encryption are common measures that are maintained. However, in emergencies, when patients are no longer able to make this decision, there is a risk that important medical information will not be accessible. Moreover, it might be very helpful to widely share medically relevant patient information among healthcare professionals to improve the quality and efficiency of treatment. Cybersecurity can thus be both supportive for privacy (understood as an aspect of autonomy) and hinder data sharing as a means for improving healthcare; therefore, it can be an obstacle to beneficence.

To analyze this problem, our contribution aims to answer two questions.

Q1. Which values are relevant for the ethics of cybersecurity in health?

Q2. What is the relation between the values at stake in cybersecurity and the four principles of medical ethics?

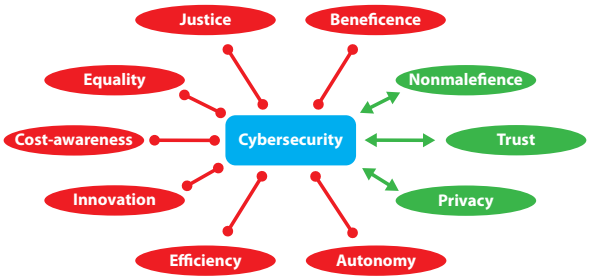
The analysis we offer relies on a conceptualization involving three classes of concepts:

(1) the principles of medical ethics;

(2) desiderata of ICT in health; and

(3) the instrumental role of cybersecurity in facilitating or hindering the achievement of each of these three desiderata.

We begin our analysis with the role of cybersecurity in healthcare by distinguishing between three types of threats based on the target of the attack: threats against information, information systems and medical devices. In a fundamental sense, however, all attacks can be described as threats to the *confidentiality, integrity and availability* of information (Anderson, 1972; Voydock and Kent, 1983), including disrupting a system such that information cannot be processed. These threats relate to four main functions of ICT systems: improving the quality and efficiency of services, protecting confidentiality, enhancing usability and protecting patients' safety. Finally, the tensions of these four desiderata to the principles of biomedical ethics are explained (Figure 2). While this involves a huge simplification of the debate, it allows us to explain in a relatively simple manner the role of



Note: Green: supportive; red: in tension

Figure 1.
Relation of health domain values to cybersecurity

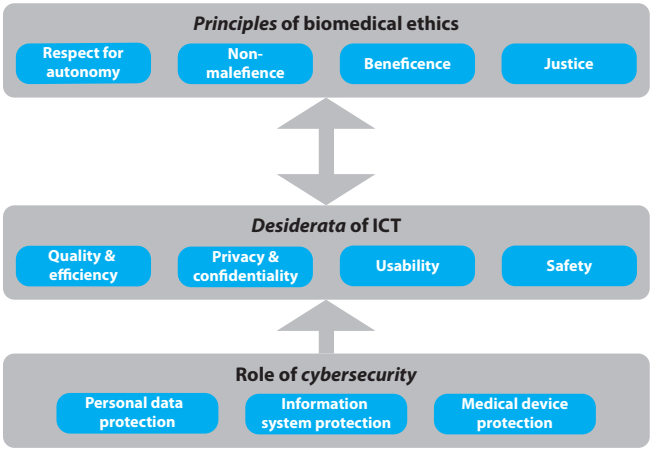


Figure 2.
Structure of the argument

cybersecurity. Our contribution is based on a review of 75 papers that were identified as being relevant for ethics in cybersecurity regarding health (Yaghmaei *et al.*, 2017).

2. Desiderata of information and communication technology and the instrumental value of cybersecurity

Cybersecurity is not an end in itself but a precondition or means of other more general functions of ICT in health. Hence, it might be possible to explain the value conflicts in cybersecurity by relating them to the most important desiderata of virtually all ICT systems. We can distinguish between them as follows:

- quality and efficiency of services;
- privacy;
- usability; and
- safety.

2.1 First desideratum: efficiency and quality of services

If one agrees that health is an important value to human beings, then a healthcare system that can provide effective and efficient help in case of medical problems is most valuable. As reported by Nancy Lorenzi (2005, p. 2), currently:

> [a]lmost every major economy in the world experiences the effects of the high cost of health care, and many, if not most, national and regional governments are in some stage of healthcare reform.

In fact, it can be said that in many countries, the reform of the healthcare system has developed into a permanent state. The development and implementation of ICT to support the provision of healthcare services is often a major part of these reforms. One of the main purposes of ICT systems in healthcare is the administration of information about patients and treatments to increase the efficiency of the healthcare system and, at the same time, to reduce its costs.

Quality, which is distinct from efficiency, refers to improvements in healthcare of qualitative and not quantitative nature. It refers, for example, to radically new services, as

opposed to deliver more of the same kind of services, with the same resources. For instance, the collection and sharing of as much health-related data as possible could be used to identify new information about diseases and possible treatments and would thus enable innovations in healthcare (Olvingson *et al.*, 2002; Vayena *et al.*, 2016). Genomic research is especially seen as a promising approach to bring about progress in public health (Caulfield *et al.*, 2008); it could even be argued that participating in biobanks is an act of solidarity (Hens *et al.*, 2011; Hoedemaekers *et al.*, 2007).

2.2 Second desideratum: privacy

McClanahan (2007, p. 69) stresses that:

> [*t*]he increased use of electronic medical records has created a substantial tension between two desirable values: the increased quality and utility of patient medical records and the protection of the privacy of the information they contain.

Privacy is an important desideratum of services in the medical domain. Privacy includes both individual privacy, the ability to control information about the self (Westin, 1967; Fried, 1970), and group privacy (Bloustein, 2003), which protects "the desire and need of people to come together, to exchange information, share feelings, make plans and act in concert to attain their objectives" (Bloustein, 2003, p. 124), particularly the exchange of information between patients and their physicians and other caregivers.

Protecting "confidentiality", i.e. preventing unauthorized information gain, is one of the main goals of cybersecurity (Anderson, 1972; Voydock and Kent, 1983). Confidentiality in the cybersecurity sense can be understood as a means to protect the privacy of both individuals and groups.

2.3 Third desideratum: usability

ICT is designed to afford usability: "[T]he degree of effectiveness, efficiency, and satisfaction with which users of a system can realize their intended task" (Roman *et al.*, 2017, p. 70). Depending on the function of the ICT item in question, users can be patients, health workers and professionals, administrators or a combination of these. Persons in all three of these categories have different degrees of ICT competences, depending on personal attitudes and socio-demographic variables (e.g. education and age) or individual capabilities, and their limitations, e.g. handicapped persons. Hence, ICT that has a high degree of usability for most people in a given demographics may have a poor degree of usability in a different demographics (Kaplan and Litewka, 2008). Usability is not entirely independent of quality and efficiency. Low usability can compromise quality and efficiency directly, e.g. when it leads to human errors or a slowing down of the processes. While it may be difficult to consider quality independently of usability, one can imagine usability as a filter that limits access to more intrinsic qualities of a service in different degrees for different kinds of users. Users who are more willing to invest time in learning how to use a service may have access to a quality that is inaccessible to other users.

2.4 Fourth desideratum: safety

For the sake of this study, safety can be defined as the reduction of health-threatening risk and risks to persons' health. *Security* in cybersecurity typically refers to the protection conferred to an entity against deliberate attacks, i.e. human causes involving malicious goals. It is clear that the security of data, information systems and devices is

necessary to protect the health of the patients that depend on them. Thus, *security* (as in cybersecurity) can be considered a means to *safety* as defined here. Safety can be distinguished from quality, in that, for example, an ICT system (e.g. an implanted drug delivery system) can both enable therapies of higher quality *and* expose the individual to new risks, e.g. in the event of a cyberattack. Usability is not entirely independent of safety. Low usability can compromise safety, quality and efficiency *directly*, e.g. when it leads to human errors.

It may be objected that confidentiality, usability and safety are all aspects of the quality of services. While this is certainly true, it is also possible to distinguish a narrower concept of quality that concerns the primary function of a service and is, at least conceptually, relatively independent from the other three desiderata. There could be improvements in the quality of care or its cost-effectiveness achieved by ICT systems that are difficult to use, place privacy at risk and generate threats to patients' safety in specific circumstances (e.g. the subject is a valuable target for economic or political reasons). Hence, it is meaningful to treat the four goals of ICT systems in questions as four distinct desiderata.

In Section 3, we therefore analyze the literature on cybersecurity in relation to the four desiderata identified above.

3. Cybersecurity as a means to information and communication technology desiderata

3.1 Quality and efficiency

First, cybersecurity is a means to protect personal information that is the prerequisite of the functioning of ICT systems designed to enhance the quality and efficiency of healthcare services. The majority of papers that we reviewed in detail are dealing with utilizing health-related electronic information or, more precisely, storing, exchanging and using patients' (big) data. As already mentioned above, the use of ICT in healthcare should support the achievement of both economic and medical objectives. Utilizing health-related electronic information efficiently requires electronic information databases such as electronic healthcare records (EHR), which are increasingly implemented in health facilities. The major advantage of these records, besides cost efficiency, is the fast and uncomplicated exchange of health-related data between organizations (van der Linden *et al.*, 2009; McGraw *et al.*, 2009) and members of different health-related professions like general practitioners, hospital doctors, nurses or paramedics. The employment of electronic information is diverse: it plays, for example, an important role in the emergency department (Ayatollahi *et al.*, 2009) or in connection with maternal and child health registries (Myhre *et al.*, 2016). Furthermore, electronic health information has a seemingly big impact on counseling and psychological therapy (Barros-Bailey and Saunders, 2010; van Allen and Roberts, 2011; Kotsopoulou *et al.*, 2015). Until now, electronic patient records have mainly been used to store "traditional" patient data such as patient's identity and demographic characteristics, recent and distant medical history, current medications, allergies and sensitivities, chronic conditions, contact information or legal preferences. Genomic data cover whole genome sequencing (Presidential Commission for the Study of Bioethical Issues, 2012), large-scale genetic data sets (Wjst, 2010) and human biobanks (Cambon-Thomsen *et al.*, 2007). Other data such as geographic information (Olvingson *et al.*, 2002) and geospatial data (Lane and Schur, 2010) might also be used in the health domain, e.g. in public health and epidemiology. Biomedical and biometric data provided by individuals and patients themselves and collected with apps and smart devices (Vayena *et al.*, 2016) also raise concerns with regard to protecting personal information. The quality element, the potential for improvement of patients' life (Devillier, 2016; Kaplan and Litewka, 2008), is often mentioned.

Some of the studies mention the security of technologies for telemedicine (Kaplan and Litewka, 2008) and in support of an independent life at home, as in the so-called ambient assisted living (AAL) systems (Ikonen and Kaasinen, 2008; Rothenpieler *et al.*, 2011; Spitalewsky *et al.*, 2013). Demographic change and its impact on the age structure of society, the availability of labor and the increase in healthcare costs will contribute to the future availability and deployment of AAL systems. Other studies focus on mobile applications such as personal health apps (e.g. Project HealthDeSign, Olmsted *et al.*, 2015) and apps for self-tracking one's own body functions and behavior (e.g. sexual and reproductive activities, Lupton, 2015), often referred to with the phrase "quantified self."

3.2 Privacy

While the primary motivation to use ICT in healthcare comes from the possibility of enhancing its quality and efficiency, the deployment of ICT in healthcare raises some ethical concern. Many of the studies that we reviewed particularly address security and privacy problems regarding EHR (i.e. Barrows and Clayton, 1996; Dong *et al.*, 2012; Ozair *et al.*, 2015; Rahim *et al.*, 2013; Stahl *et al.*, 2014). Different approaches of how to deal with security and privacy could be identified, such as solutions based on technology (for biometric authentication, e.g. Rodrigues and Santos, 2013, and for secure systems, e.g. Xiao *et al.*, 2008) and ethical guidelines (i.e. Buckovich *et al.*, 1999; The Academy of Medical Sciences, 2017). Security issues, among other factors, could lead to another crucial issue that was mentioned in 28 studies: the loss of control. The first type of issue is related to concerns regarding access control, which comprises everything from an unclear data access authorization (Dong *et al.*, 2012; Stahl *et al.*, 2014) over lacking some control (Ikonen and Kaasinen, 2008; Motti and Caine, 2015; Olmsted *et al.*, 2015; Olvingson *et al.*, 2002) to a complete loss of control with regard to personal information (Barrows and Clayton, 1996; Caulfield *et al.*, 2008). The consequence could be unauthorized access by others (Buckovich *et al.*, 1999; Greenbaum *et al.*, 2011; Myhre *et al.*, 2016), e.g. in a professional medical context (Ayatollahi *et al.*, 2009; Caldicott and Manning, 2013; McGraw *et al.*, 2009; van Allen and Roberts, 2011; Wallace, 2015; Wang *et al.*, 2013; Xiao *et al.*, 2008). The other type is the loss of control over one's own data (Barrows and Clayton, 1996; Caulfield *et al.*, 2008; Mascalzoni *et al.*, 2015). This is noticeable regarding a lack of possibilities to manage one's own data (Bourret and Pestana, 2015; Thilakanathan *et al.*, 2016), a lack of control over the concrete use of data (Greenbaum *et al.*, 2011; Ienca and Haselager, 2016; Rodrigues and Santos, 2013; Vayena *et al.*, 2016) and, in the worst case, the risk of losing ownership of one's own data (Kluge, 2011). This loss can be a risk to the empowerment of patients (Bourret and Pestana, 2015).

The less security and control one has over one's own data, the more urgent the ethical issue of misuse of data becomes, as discussed on different levels in 41 studies. In particular, data theft (i.e. Buckovich *et al.*, 1999; Myhre *et al.*, 2016; Ozair *et al.*, 2015; Thilakanathan *et al.*, 2016) and thus identity theft (Rodrigues and Santos, 2013; Rothenpieler *et al.*, 2011) are crucial issues. However, the most important risks of misuse of data are the disclosure of information (mentioned by 32 papers, i.e. McGraw *et al.*, 2009; Wjst, 2010) and a possible identification via the data (mentioned by 14 studies, among others Lane and Schur, 2010; The Academy of Medical Sciences, 2017), which may increase the risk of surveillance (Mulligan and Schneider, 2011; Ozair *et al.*, 2015; Rothenpieler *et al.*, 2011). The stated issues seem to have at least some effect on confidentiality (21 studies outline confidentiality and trust issues). On the one hand, stakeholders show a lack of trust with regard to technologies (Rahim *et al.*, 2013; Saigí-Rubió *et al.*, 2016) and security systems (Olvingson *et al.*, 2002; Tieu *et al.*, 2015). On the other hand, trust in professionals and medical staff is also an issue (Ayatollahi *et al.*,

2009; Williams, 2008), and confidentiality seems to be crucial (Caldicott and Manning, 2013; Wallace, 2015), especially in counseling settings (Barros-Bailey and Saunders, 2010; Kotsopoulou *et al.*, 2015; van Allen and Roberts, 2011). It is generally possible to (re-)identify people (e.g. their health status, relationship link, dispositions) based on genetic information (i.e. Lowrance, 2006; Vayena *et al.*, 2016; Wright *et al.*, 2013) and to commercialize this knowledge (Cambon-Thomsen *et al.*, 2007; Lupton, 2015).

3.3 Safety

Six sources discuss the risk of hacking and other forms of attacks (Motti and Caine, 2015; Mulligan and Schneider, 2011; Tieu *et al.*, 2015), which could directly affect the physical and psychological safety of individuals (Camara *et al.*, 2015; Ienca and Haselager, 2016; Altawy and Youssef, 2016). In addition to trade-offs between quality/efficiency vs privacy/confidentiality, the design of implantable medical devices illustrates better than other health-related ICT contexts the trade-offs of both former desiderata against safety (Table I). The incorporation of more extended communication and networking functions, known as telemetry, leads to improvements in quality and cost-effectiveness, e.g. patients can move freely in their homes, while healthcare providers can constantly monitor them (Camara *et al.*, 2015; Altawy and Youssef, 2016).

However, this is a "vulnerable communication channel," which "makes it easier to attack the device" and "could potentially allow an adversary to monitor and modify the implant without necessarily being close to the victim" (Camara *et al.*, 2015, pp. 272-273). This also compromises quality of services with implications on safety, e.g. "if the information sent by

Type of attacks	Representative IMD types	Consequences (by IMD type)	Technical trade-offs and constraints
Impersonation (adversary can send commands, modify message in transit to IMD, or block them). More specifically: reprogramming therapies on ICD inducing a state of shock to the patient depleting the battery and render the device inoperative	Cardiac implanted device →	Hearth failure, tachycardia, bradycardia, cardiac arrhythmia	Battery lifetime (quality)
	Neurostimulator →	Inappropriate stimulation, failure to stimulate, tremors and spasms, neuronal effects	Answering time (quality)
	Drug delivery system →	Loss of pain reliefs, injury, inappropriate dosage, inappropriate timing	Accessibility in emergency situations (usability and safety), emergency authentication
	Cochlear implant →	Deafness, background noise, ringing, distraction or confusion	Higher likelihood of errors and necessity of maintenance (quality)
Denial of service attack: disable therapies on ICD		Undergo a surgical procedure to have the IMD replaced	
Passive adversary with capability to listen to the communications between IMDs and programmers		Breach of privacy *Security* (as in cybersecurity) can be considered a means to *safety* defined in this sense	

Sources: Camara *et al.* (2015); Altawy and Youssef (2016)

Table I.
Cybersecurity of implantable medical devices

the implant to the programmer is altered, the doctor might make a wrong decision" (Camara *et al.*, 2015, p. 273).

3.4 Usability

The analysis of the literature, particularly on electronic health records, telemedicine and AAL technologies, highlights difficulties regarding usability (Roman *et al.*, 2017; Kaplan and Litewka, 2008; Spitalewsky *et al.*, 2013; Young *et al.*, 2014) and the importance of acceptance of ICT systems by their users (Saigí-Rubió *et al.*, 2016; Tieu *et al.*, 2015). One example of a usability issue is the aforementioned trade-off between the usability of an implant outside a medical environment and its vulnerability to cybersecurity attacks. Another one, again in the context of implantable devices, is the fact that authentication may be problematic in emergency situations (Camara *et al.*, 2015; Altawy and Youssef, 2016).

Because usability can differ for different demographics, there is a tight connection between this desideratum and one of the outstanding ethical issues concerning ICT in health, emerging from our review: the fact that vulnerable groups and those with special needs must be taken into particular consideration. Because of the "digital divide," people who have little or no experience with the application of ICT can face disadvantages regarding health-related services (Chang *et al.*, 2004). This also applies to people with limited health literacy (e.g. in case of use of online portals, Tieu *et al.*, 2015). The literature shows that the elderly form a group with special needs and interests, which could present a barrier for the adoption of health-related technologies (Devillier, 2016; Young *et al.*, 2014). People with dementia, Alzheimer's or other cognitive handicaps present a special case (i.e. Batchelor *et al.*, 2012).

3.5 Instrumental role of cybersecurity

Cybersecurity measures are a means to ensure the reliability of ICT, which is a key requisite for the quality, efficiency and safety and privacy of health services. In 26 studies addressing technical security issues in health contexts, difficulties concerning reliability of systems (Ikonen and Kaasinen, 2008; Spitalewsky *et al.*, 2013) and reliability of data (i.e. Ozair *et al.*, 2015) have been mentioned. Threats to data integrity are unauthorized modification (Barrows and Clayton, 1996; Stahl *et al.*, 2014; Wang *et al.*, 2013), manipulation (Kaplan and Litewka, 2008; Kluge, 2011) or sabotage of data (Williams, 2008). Cybersecurity involves trade-offs regarding quality of ICT, as shown by the literature on implantable medical devices (Table I): encryption and authentication, e.g., slow down device response and indicate higher energy consumption. The latter has implications on battery and thus device life, which, in turn, has implications on cost-effectiveness and safety because surgery is required to replace such devices.

Cybersecurity's relation to usability is also multifaceted. On the one hand, cybersecurity can be a *hindrance* to usability. This holds mainly for two reasons: for humans, adhering to policies that are necessary to keep data, systems and devices secure, which normally takes resources such as time and mental efforts (Tieu *et al.*, 2015, related to dementia and remembering passwords see Batchelor *et al.*, 2012). Second, cybersecurity technologies tend to reduce the immediacy with which the data, system or device can be used for its primary function as shown by the example of authentication for implantable medical devices (Camara *et al.*, 2015; Altawy and Youssef, 2016).

On the other hand, poor usability can be an indirect cybersecurity threat. For example (outside cybersecurity), aggressive warning messages in AAL lead users to deactivate security messages (Rothenpieler *et al.*, 2011). Similarly, in the cybersecurity

context, when security is a hindrance to usability, it may backfire, e.g. users may look for workarounds such as writing complex passwords on a post-it to easily access them.

Summing up, it seems that the four desiderata explored here, namely, quality and efficiency of services, privacy, usability of health-related ICT systems and safety, are related as in a pentalemma, where you cannot simultaneously advance all of them through cybersecurity. For example, cybersecurity protects systems that produce, connect and make large amounts of personal data accessible while ensuring their integrity and completeness. This, however, makes privacy harder to protect. If cybersecurity also includes tools for protecting privacy, they must reduce the information in the data or its accessibility. If one wants to have *both* high-quality services *and* privacy protection, data should be accessible for some and inaccessible for others, i.e. one needs authorization systems but these also reduce usability.

4. Cybersecurity and principles of biomedical ethics

4.1 Four principles of biomedical ethics

The "Principles of Biomedical Ethics," first published in 1977 by Tom L. Beauchamp and James F. Childress, is a classic text in biomedical ethics (Beauchamp and Childress, 2013). The core features of this principlism are to identify four moral principles (autonomy, non-maleficence, beneficence and justice) pertinent to a particular moral situation and to use specification, balancing and (deductive) application to create a bridge between the moral situation and the relevant principles.

Principlism is not undisputed in bioethics (Clouser and Gert, 1990; Hine, 2011). Nevertheless, principlism remains highly influential among bioethicists and practitioners (Reijers *et al.*, 2017). Hence, we would like to use principlism as a starting point of our ethical analysis concerning cybersecurity in health.

The four principles of biomedical ethics are *respect for autonomy*, *non-maleficence*, *beneficence* and *justice*. Beauchamp and Childress' definitions can be summarized as follows:

(1) *Respect for autonomy* involves the right for an individual (patient) to make his or her own choice, particularly for medical decisions. It involves the right to be informed about therapeutic and diagnostic options in an appropriate way.

(2) *Non-maleficence* can be derived from the classic quote "above all, do no harm," as stated in the Hippocratic Oath. It involves the duty to make pertinent risk-benefit assessments and to minimize risks to patients (and others) because of medical action (or omission).

(3) *Beneficence* requires acting with the best interest of the other in mind. It reflects the basic moral motivation of medical acting, namely, to improve the health status and quality of life of your patient.

(4) *Justice* emphasizes fairness and equality among individuals. It requires going beyond the mere interaction between individual patients and medical professionals and taking a holistic point of view, particularly with respect to distributive justice of scarce goods.

4.2 Relations between information and communication technology desiderata and the four principles

Quality and efficiency are mostly related to beneficence. A more cost-effective system can potentially help more people. Quality improvements can help people who could not have been helped in the past. Moreover, even if quality innovations may initially not be cost-

effective, often they become more affordable with time and tend to augment the number of persons helped and treated in the long term.

Safety is mostly related to non-maleficence. Once ICT services promoting quality and efficiency are in place, the failure to guarantee their reliability can lead to harming individuals. Higher information processing or communication capabilities can do more harm than more primitive systems with less capabilities, even if the former are potentially able to confer greater benefits (or the same benefit to more people) than the latter.

Privacy is mostly related to autonomy and non-maleficence. Some cybersecurity measures are meant to guarantee the privacy of information and communication within healthcare. Non-maleficence is at stake because violations of privacy can cause reputational harm, discrimination and all those other risks to which a blackmailed subject may expose him or herself and those who depend on the subject's decisions.

Moreover, privacy is a precondition of autonomy. The connection between privacy and autonomy is more organic. It has been argued that privacy is essential for autonomy in the sense of individuality (Bloustein, 2003, p. 42):

> The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny [. . .] merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual.

Usability is mostly related to justice, but it is also related to non-maleficence and autonomy. There is a complex relation between usability, justice and each of the other principles. A system may enhance the *autonomy* of some users, those who are able to navigate a more complex system and express their preferences through it, but it may at the same time reduce the autonomy of health-illiterate or ICT-challenged ones. Moreover, poor usability may compromise safety, for example, information in a medical implant may be harder to retrieve in emergency situations. It may *unequally* affect the security of different populations in different circumstances. A design choice that enhances the autonomy or safety of some of its users while reducing that of others may be considered unjust because it distributes benefits unequally, especially if those negatively affected belong to vulnerable populations, which are already in a situation of disadvantage.

5. Conflicts of moral principles in cybersecurity

Having explained the relation between ICT desiderata and the four principles of medical ethics, it is now possible to map trade-offs between the goals of cybersecurity into conflicts between the four principles of medical ethics.

5.1 Prioritizing beneficence and autonomy at the expense of justice

Suppose that cybersecurity protections in healthcare are designed to optimize the quality and efficiency of services and the privacy of information and confidentiality of communication, while sacrificing usability and safety. As shown above, a system maximizing the amount of data produced and analyzed could be responsive to the individual privacy preferences of patients, thus enhancing their autonomy and allocating resources efficiently, which may benefit more people (beneficence). But a system capable of achieving this will tend to be quite complex and, as such, compromises usability for certain demographics, in contrast or even contradiction to the justice principle.

5.2 Prioritizing beneficence and (informational self-determination) autonomy at the expense of non-maleficence

Consider again a highly networked, data-intensive information system in healthcare, which is designed to benefit people with better and more cost-effective services, while respecting their autonomy. If the system involves complex, granular, stratified authorization systems, requiring complex passwords, it may invite workarounds which undermine cybersecurity defenses. This generates exposure to passive and active attackers, who may interfere with a device or gain access to confidential information, which is in conflict with the principle of non-maleficence. In relation to implantable medical devices, a system with extended networking capabilities and privacy protections may reduce usability in critical situations (authorization issues) and safety (e.g. battery life issues), which is also in tension with the principle of non-maleficence.

5.3 Prioritizing beneficence, justice and non-maleficence at the expense of autonomy and non-maleficence

Suppose that the quality and efficiency of services are optimized, together with usability and sacrificing privacy, e.g. a system that makes extensive use of electronic health records and extensive surveillance of patients through data generated by medical devices with good protection of data integrity and accessibility but poor protection for confidentiality and privacy. Such a design may comply with some aspects of the principle of beneficence (data-intensive services) and some aspects of non-maleficence (increased patient surveillance), but sacrifice autonomy (patient surveillance and privacy violations) and other aspects of non-maleficence (harmful privacy violations). Incidentally, such a design may be compatible with justice only because it "levels down" privacy and autonomy.

5.4 Prioritizing non-maleficence and (privacy-related) autonomy at the expense of beneficence and autonomy

Consider a system of medical health records optimized to promote privacy and safety. The most extreme form of this would be a system minimizing data collection, data sharing, communication and networking. Such a system may be able to avoid privacy breaches and impersonation and denial of service attacks, thus avoiding device malfunctions. It would be responsive to the principle of non-maleficence and also of autonomy, i.e. it protects privacy, which is crucial for autonomy.

Such a design, however, could not be used for providing data intensive services, which may involve a sacrifice in quality and/or cost-effectiveness. This is contrary to the principle of beneficence. In the context of implantable medical devices, maximizing privacy and safety leads to sacrificing certain aspects of usability (e.g. no wireless monitoring) with implications on autonomy.

5.5 Prioritizing for justice at the expense of autonomy and non-maleficence

A design choice may promote quality and efficiency while equalizing safety and privacy for different demographics. Consider an electronic health record with a relatively simple authentication system and just one privacy setting for all. Complex authentication systems would be avoided too. It may be more suitable for patients from certain demographics (e.g. elderly or illiterate), who may actually gain autonomy because of a system that offers few personalization options and is thus simple to use. Less sophisticated ICT users would also be less tempted to find workarounds to security systems, so the system may achieve a more even level of security. The design may achieve a more equal distribution of benefits because

it would be easier for otherwise disadvantaged users to take advantage of it. Such a simple system would be maximally compatible with justice, but it would be incompatible with services that guarantee informational self-determination. It would also conflict with non-maleficence because it would feature weak authentication, which could put the privacy of the most vulnerable individuals at risk.

6. Conclusion: How should one set priorities between conflicting principles?

The preceding analysis shows that trade-offs involved in design choices for cybersecurity systems map into conflicts between the four principles of medical ethics. We use the concept of a "conflict" to describe the fact that different principles (beneficence, non-maleficence, autonomy and justice) point in different directions. We use the concept of a "trade-off" to describe the extent to which a design choice can satisfy each principle. The above analysis deals with the most extreme cases for the purpose of illustration. For example, the design choice described in Section 5.1 tries to maximally satisfy the beneficence and autonomy principles, which leads to sacrificing justice. Conversely, the design choice described in Section 5.5 tries to maximally satisfy justice with a cost in terms of the degree to which principles of autonomy and non-maleficence are satisfied. As the design choices discussed in Sections 5.3 and 5.4 show, the trade-off can also be between different *ways* of satisfying the same principle. For example, the design in Section 5.3 fulfills the principle of non-maleficence by enhancing patient surveillance but makes the patient vulnerable to another kind of harm because of reduced privacy. The design in Section 5.4 fulfills the autonomy principle with respect to privacy (which is an enabler of autonomy) but not with respect to usability (which is an enabler too). Of course, real-world choices do not have to be so extreme because designers will try to partially accommodate all principles without fully sacrificing any of them. However, the trade-offs seem unavoidable.

Principlism does not provide priority rules for balancing the four principles when they conflict. This is left to the individual wisdom of ethical decision-makers (e.g. physicians, administrators) as no formula is given to make decisions. However, the departure from the tradition of medical beneficence and the "discovery" of patient autonomy is possibly the most significant evolution in medical ethics since at least the second half of 20th century (Faden and Beauchamp, 1986, pp. 75-100). In this tradition, the emphasis is on *being respected as an autonomous individual*, rather than on the (arguably more demanding) conditions of *being autonomous,* involving actual independence and authenticity in the subjects involved (Faden and Beauchamp, 1986, pp. 7-8). It may be possible to ask whether this idea of a priority of the principle of respect for autonomy, conceived in this way, is normatively appropriate and whether it *de facto* represents a dominant view among experts of this domain not only concerning the role of the patient vis-a-vis a physician but also of the user of ICT in health vis-a-vis cybersecurity.

With reference to cybersecurity of personal data and information systems, respect for autonomy may initially appear enhanced by a system that tries to optimize for quality/efficiency and privacy/confidentiality while sacrificing usability and safety; however, this is objectionable. Except in a formal sense, such design distributes the preconditions for autonomy in a somewhat unequal way. This system will only enhance the autonomy of some people, namely, those with the competences and abilities required to be able to use and take advantage of such systems and protect themselves well against cybersecurity risks.

A system sacrificing privacy tends to be incompatible with autonomy because it enables privacy violations with negative impact on autonomy across a wide-range of social contexts.

Finally, a system sacrificing quality and usability would also be problematic for autonomy, e.g. consider implantable devices. A design that minimizes networking and communication

capabilities may afford better protection of privacy (against eavesdroppers) and safety (against life- or health-threatening manipulations or malfunctions). However, it will have to sacrifice usability in a way that it reduces autonomy, e.g. in relation to the possibility for a patient to leave medical environments and have a more autonomous life outside.

We believe that additional research, both empirical and normative, is required to determine if respect for autonomy should be given more importance than other principles and whether this is in fact a tendency in the field. Even if respect for autonomy is given more importance, it may be questioned whether the principle of respect for autonomy enjoys the same importance in "common morality" as it appears to have among practitioners of ethics or policy-makers in the field. It is yet another question whether this moral view is correct, irrespective of its popularity. Finally, the analysis here suggests that it is important to investigate aspects of autonomy that are not associated with privacy protection, but with the usability of ICT in healthcare.

References

Altawy, R. and Youssef, A.M. (2016), "Security tradeoffs in cyber physical systems: a case study survey on implantable medical devices", *IEEE Access*, Vol. 4, pp. 959-979, available at: https://doi.org/10.1109/ACCESS.2016.2521727

Anderson, J.P. (1972), "Information security in a multi-user computer environment", *Advances in Computers*, Vol. 12, pp. 1-36.

Ayatollahi, H., Bath, P.A. and Goodacre, S. (2009), "Accessibility versus confidentiality of information in the emergency department", *Emergency Medicine Journal*, Vol. 26 No. 12, pp. 857-860, available at: https://doi.org/10.1136/emj.2008.070557

Barros-Bailey, M. and Saunders, J.L. (2010), "Ethics and the use of technology in rehabilitation counseling", *Rehabilitation Counseling Bulletin*, Vol. 53 No. 4, pp. 255-259, available at: https://doi.org/10.1177/0034355210368867

Barrows, R.C. and Clayton, P.C. (1996), "Privacy, confidentiality, and electronic medical records", *Journal of the American Medical Informatics Association*, Vol. 3 No. 2, pp. 139-148.

Batchelor, R., Bobrowicz, A., Mackenzie, R. and Milne, A. (2012), "Challenges of ethical and legal responsibilities when technologies' uses and users change: social networking sites, decision-making capacity and dementia", *Ethics and Information Technology*, Vol. 14 No. 2, pp. 99-108, available at: https://doi.org/10.1007/s10676-012-9286-x

Beauchamp, T.L. and Childress, J.F. (2013), *Principles of Biomedical Ethics*, 7th ed., Oxford University Press, New York, NY.

Bloustein, E.J. (2003), *Individual and Group Privacy*, Routledge, New Brunswick.

Bourret, C. and Pestana, O. (2015), "Information systems and patients' empowerment around patients' pathways: the French and the Portuguese scenarios", *Qualitative and Quantitative Methods in Libraries*, Vol. 4, pp. 767-773.

Buckovich, S.A., Rippen, H.E. and Rozen, M.J. (1999), "Driving toward guiding principles: a goal for confidentiality, and security of health information", *Journal of the American Medical Informatics Association*, Vol. 6 No. 2, pp. 122-133.

Caldicott, D.F. and Manning, K. (2013), "A guide to confidentiality in health and social care: treating confidential information with respect", Health and Social Care In-formation Center, available at: http://content.digital.nhs.uk/media/12822/Guide-to-confidentialityin-health-and-socialcare/pdf/HSCIC-guide-to-confidentiality.pdf

Camara, C., Peris-Lopez, P. and Tapiador, J.E. (2015), "Security and privacy issues in implantable medical devices: a comprehensive survey", *Journal of Biomedical Informatics*, Vol. 55, pp. 272-289, available at: https://doi.org/10.1016/j.jbi.2015.04.007

Cambon-Thomsen, A., Rial-Sebbag, E. and Knoppers, B.M. (2007), "Trends in ethical and legal frameworks for the use of human biobanks", *European Respiratory Journal*, Vol. 30 No. 2, pp. 373-382, available at: https://doi.org/10.1183/09031936.00165006

Caulfield, T., McGuire, A.L., Cho, M., Buchanan, J.A., Burgess, M.M., Danilczyk, U., Diaz, C.D., Fryer-Edwards, K., Green, S.K., Hodosh, M.A., Juengst, E.T., Kaye, J., Kedes, L., Knoppers, B.M., Lemmens, T., Meslin, E.M., Murphy, J., Nussbaum, R.L., Otlowski, M., Pullman, D., Ray, P.N., Sugarman, J. and Timmons, M. (2008), "Research ethics recommendations for whole-genome research: consensus statement", *PLoS Biology*, Vol. 6 No. 3, pp. 430-435, available at: https://doi.org/10.1371/journal.pbio.0060073

Chang, B.L., Bakken, S., Brown, S.S., Houston, T.K., Kreps, G.L., Kukafka, R., Safran, C. and Stavri, P.Z. (2004), "Bridging the digital divide: reaching vulnerable populations", *Journal of the American Medical Informatics Association*, Vol. 11 No. 6, pp. 448-457, available at: https://doi.org/10.1197/jamia.M1535

Clouser, K.D. and Gert, B. (1990), "A critique of principlism", *Journal of Medicine and Philosophy*, Vol. 15 No. 2, pp. 219-236, available at: https://doi.org/10.1093/jmp/15.2.219

Devillier, N. (2016), "Ageing, well-being and technology: from quality of life improvement to digital rights management: a French perspective", *Proceedings of the 2016 ITU Kaleidoscope Academic Conference – ICTs for a Sustainable World (ITU WT)*, pp. 41-47.

Dong, N., Jonker, H. and Pang, J. (2012), "Challenges in eHealth: from enabling to enforcing privacy", in Liu, Z. and Wassyng, A. (Eds), *Foundations of Health Informatics Engineering and Systems*, Springer, Berlin, Heidelberg, Vol. 7151, pp. 195-206, available at: https://doi.org/10.1007/978-3-642-32355-3_12

ENISA (2016), "Smart hospitals. Security and resilience for smart health service and infrastructures", European Union Agency for Network and Information Security, available at: www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Faden, R.R. and Beauchamp, T.L. (1986), *A History and Theory of Informed Consent*, Oxford University Press, New York, NY.

Fried, C. (1970), *An Anatomy of Values: Problems of Personal and Social Choice*, Harvard University Press, Cambridge, MA.

Greenbaum, D., Sboner, A., Mu, X.J. and Gerstein, M. (2011), "Genomics and privacy: implications of the new reality of closed data for the field", *PLoS Computational Biology*, Vol. 7 No. 12, available at: https://doi.org/10.1371/journal.pcbi.1002278

Hens, K., Lévesque, E. and Dierickx, K. (2011), "Children and biobanks: a review of the ethical and legal discussion", *Human Genetics*, Vol. 130 No. 3, pp. 403-413, available at: https://doi.org/10.1007/s00439-011-1031-8

Hine, K. (2011), "What is the outcome of applying principlism?", *Theoretical Medicine and Bioethics*, Vol. 32 No. 6, pp. 375-388, available at: https://doi.org/10.1007/s11017-011-9185-x

Hoedemaekers, R., Gordijn, B. and Pijnenburg, M. (2007), "Solidarity and justice as guiding principles in genomic research", *Bioethics*, Vol. 21 No. 6, pp. 342-350, available at: https://doi.org/10.1111/j.1467-8519.2007.00562.x

Ienca, M. and Haselager, P. (2016), "Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity", *Ethics and Information Technology*, Vol. 18 No. 2, pp. 117-129, available at: https://doi.org/10.1007/s10676-016-9398-9

Ikonen, V. and Kaasinen, E. (2008), "Ethical assessment in the design of ambient assisted living", in Karshmer, A.I., Nehmer, J., Raffler, H. and Tröster, G. (Eds), Dagstuhl Seminar Proceedings Assisted Living Systems – Models, Architectures and Engineering Approaches, available at: http://drops.dagstuhl.de/opus/volltexte/2008/1462

Kaplan, B. and Litewka, S. (2008), "Ethical challenges of telemedicine and telehealth", *Cambridge Quarterly of Healthcare Ethics*, Vol. 17 No. 4, pp. 401-416, available at: https://doi.org/10.1017/S0963180108080535

Kluge, E.-H.W. (2011), "E-Health promises and challenges: some ethical considerations", in Borycki, E. M., BartleClar, J.A., Househ, M.S., Kuziemsky, C.E. and Schraa, E.G. (Eds), *International Perspectives in Health Informatics. Studies in Health Technology and Informatics 164*, IOS Press, Amsterdam, pp. 148-153.

Kotsopoulou, A., Melis, A., Koutsompou, V.-I. and Karasarlidou, C. (2015), "E-Therapy: the ethics behind the process", *Procedia Computer Science*, Vol. 65, pp. 492-499, available at: https://doi.org/10.1016/j.procs.2015.09.120

Lane, J. and Schur, C. (2010), "Balancing access to health data and privacy: a review of the issues and approaches for the future", *Health Services Research*, Vol. 45, pp. 1456-1467, available at: https://doi.org/10.1111/j.1475-6773.2010.01141.x

Lorenzi, N.M. (2005), "Introduction", in Lorenzi, N.M., Ash, J.S., Einbinder, J., McPhee, W. and Einbinder, L. (Eds), *Transforming Health Care through Information*, 2nd ed., Springer, New York, NY, pp. 2-6.

Lowrance, W.W. (2006), "Privacy, confidentiality, and identifiability in genomic research: discussion document for workshop convened by the national human Ge-nome research institute, Bethesda, 3-4 October", available at: www.genome.gov/pages/about/od/reportspublications/identifiabilityworkshopwhitepaper.pdf

Lupton, D. (2015), "Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps", *Culture Health and Sexuality*, Vol. 17 No. 4, pp. 440-453, available at: https://doi.org/10.1080/13691058.2014.920528

McClanahan, K. (2007), "Balancing good intentions: protecting the privacy of electronic health information", *Bulletin of Science, Technology and Society*, Vol. 28 No. 1, pp. 69-79, available at: https://doi.org/10.1177/0270467607311485

McGraw, D., Dempsey, J.X., Harris, L. and Goldman, J. (2009), "Privacy as an enabler, not an impediment: building trust into health information exchange", *Health Affairs*, Vol. 28 No. 2, pp. 416-427, available at: https://doi.org/10.1377/hlthaff.28.2.416

Mascalzoni, D., Dove, E.S., Rubinstein, Y., Dawkins, H.J.S., Kole, A., McCormack, P., Woods, S., Riess, O., Schaefer, F., Lochmüller, H., Knoppers, B.M. and Hansson, M. (2015), "International charter of principles for sharing bio-specimens and data", *European Journal of Human Genetics*, Vol. 23 No. 6, pp. 721-728, available at: https://doi.org/10.1038/ejhg.2014.197

Motti, V.G. and Caine, K. (2015), "Users' privacy concerns about wearables: impact of form factor, sensors and type of data collected", in Brenner, M., Christin, N., Johnson, B. and Rohloff, K. (Eds), *Financial Cryptography and Data Security (FC 2015), 8976*, Springer, Berlin, pp. 231-244.

Mulligan, D.K. and Schneider, F.B. (2011), "Doctrine for cybersecurity", *Daedalus*, Vol. 140 No. 4, pp. 70-92.

Myhre, S.L., Kaye, J., Bygrave, L.A., Aanestad, M., Ghanem, B., Mechael, P. and Frøen, J.F. (2016), "eRegistries: governance for electronic maternal and child health registries", *BMC Pregnancy and Childbirth*, Vol. 279 No. 16, available at: https://doi.org/10.1186/s12884-016-1063-0

Olmsted, M.G., Massoudi, B.L. and Zhang, Y. (2015), "What consumers want in personal health applications: findings from project HealthDesign", *Personal and Ubiquitous Computing*, Vol. 19 No. 1, pp. 79-83, available at: https://doi.org/10.1007/s00779-014-0811-2

Olvingson, C., Hallberg, J., Timpka, T. and Lindqvist, K. (2002), "Ethical issues in public health informatics: implications for system design when sharing geographic information", *Journal of Biomedical Informatics*, Vol. 35 No. 3, pp. 178-185, available at: https://doi.org/10.1016/S1532-0464(02)00527-0

Ozair, F.F., Jamshed, N., Sharma, A. and Aggarwal, P. (2015), "Ethical issues in electronic health records: a general overview", *Perspectives in Clinical Research*, Vol. 6 No. 2, pp. 73-76, available at: https://doi.org/10.4103/2229-3485.153997

Presidential Commission for the Study of Bioethical Issues (2012), *Privacy and Progress in Whole Genome Sequencing*, Presidential Commission for the Study of Bioethical Issues, Washington, DC.

Rahim, F.A., Ismail, Z. and Samy, G.N. (2013), "Information privacy concerns in electronic healthcare records: a systematic literature review", 2013 IEEE International Conference on Research and Innovation in Information Systems (ICRIIS), pp. 504-509, available at: https://doi.org/10.1109/ICRIIS.2013.6716760

Reijers, W., Wright, D., Brey, P., Weber, K., Rodrigues, R., O'Sullivan, D. and Gordijn, B. (2017), "Methods for practising ethics in research and innovation: a literature review, critical analysis and recommendations", *Science and Engineering Ethics*, Vol. 24 No. 5, pp. 1437-1481, available at: https://doi.org/10.1007/s11948-017-9961-8

Rodrigues, P. and Santos, H. (2013), "Health users' perception of biometric authentication technologies", in Rodrigues, P.P., Pechenizkiy, M., Gama, J., Correia, R.C., Liu, J., Traina, A., Lucas, P. and Soda, P. (Eds), *2013 IEEE 26th International Symposium on Computer-Based Medical Systems (CBMS)*, pp. 320-325, available at: https://doi.org/10.1109/CBMS.2013.6627809

Roman, L.C., Ancker, J.S., Johnson, S.B. and Senathirajah, Y. (2017), "Navigation in the electronic health record: a review of the safety and usability literature", *Journal of Biomedical Informatics*, Vol. 67, pp. 69-79, available at: https://doi.org/10.1016/j.jbi.2017.01.005

Rothenpieler, P., Becker, C. and Fischer, S. (2011), "Privacy concerns in a remote monitoring and social networking platform for assisted living", in Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R. and Zhang, G. (Eds), *Privacy and Identity Management for Life*, Springer, Berlin and Heidelberg, Vol. 352, pp. 219-230, available at: https://doi.org/10.1007/978-3-642-20769-3_18

Saigí-Rubió, F., Jiménez-Zarco, A. and Torrent-Sellens, J. (2016), "Determinants of the intention to use telemedicine: evidence from primary care physicians", *International Journal of Technology Assessment in Health Care*, Vol. 32 Nos 1/2, pp. 29-36, available at: https://doi.org/10.1017/S0266462316000015

Spitalewsky, K., Rochon, J., Ganzinger, M. and Knaup, P. (2013), "Potential and requirements of IT for ambient assisted living technologies: results of a Delphi study", *Methods of Information in Medicine*, Vol. 52 No. 3, pp. 231-238, available at: https://doi.org/10.3414/ME12-01-0021

Stahl, B.C., Doherty, N.F., Shaw, M. and Janicke, H. (2014), "Critical theory as an approach to the ethics of information security", *Science and Engineering Ethics*, Vol. 20 No. 3, pp. 675-699, available at: https://doi.org/10.1007/s11948-013-9496-6

The Academy of Medical Sciences (2017), "Personal data for public good: using health information in medical research", available at: https://acmedsci.ac.uk/policy/policy-projects/personal-data

Thilakanathan, D., Calvo, R.A., Chen, S., Nepal, S. and Glozier, N. (2016), "Facilitating secure sharing of personal health data in the cloud", *JMIR Medical Informatics*, Vol. 4 No. 2, pp. 56-73, available at: https://doi.org/10.2196/medinform.4756

Tieu, L., Sarkar, U., Schillinger, D., Ralston, J.D., Ratanawongsa, N., Pasick, R. and Lyles, C.R. (2015), "Barriers and facilitators to online portal use among patients and caregivers in a safety net health care system: a qualitative study", *Journal of Medical Internet Research*, Vol. 17 No. 12, p. e275, available at: https://doi.org/10.2196/jmir.4847

Van Allen, J. and Roberts, M.C. (2011), "Critical incidents in the marriage of psychology and technology: a discussion of potential ethical issues in practice, education, and policy", *Professional Psychology-Research and Practice*, Vol. 42 No. 6, pp. 433-439, available at: https://doi.org/10.1037/a0025278

van der Linden, H., Kalra, D., Hasman, A. and Talmon, J. (2009), "Inter-organizational future proof EHR systems: a review of the security and privacy related issues", *International Journal of Medical Informatics*, Vol. 78 No. 3, pp. 141-160, available at: https://doi.org/10.1016/j.ijmedinf.2008.06.013

Vayena, E., Gasser, U., Wood, A., O'Brien, D. and Altman, M. (2016), "Elements of a new ethical framework for big data research", *Washington and Lee Law Review*, Vol. 72 No. 3, pp. 420-441.

Voydock, V.L. and Kent, S.T. (1983), "Security mechanisms in high-level network protocols", *ACM Computing Surveys*, Vol. 15 No. 2, pp. 135-171.

Wallace, I.M. (2015), "Is patient confidentiality compromised with the electronic health record? A position paper", *CIN: Computers, Informatics, Nursing*, Vol. 33 No. 2, pp. 58-62, available at: https://doi.org/10.1097/CIN.0000000000000126

Wang, J., Zhang, Z., Xu, K., Yin, Y. and Guo, P. (2013), "A research on security and privacy issues for patient related data in medical organization system", *International Journal of Security and Its Applications*, Vol. 7 No. 4, pp. 287-298.

Westin, A.F. (1967), *Privacy and Freedom*, 1st ed., Atheneum, New York, NY.

Williams, P.A.H. (2008), "In a 'trusting' environment, everyone is responsible for information security", *Information Security Technical Report*, Vol. 13 No. 4, pp. 207-215. availble at: https://doi.org/10.1016/j.istr.2008.10.009.

Wjst, M. (2010), "Caught you: threats to confidentiality due to the public release of Large-Scale genetic data sets", *BMC Medical Ethics*, Vol. 11 No. 11, available at: https://doi.org/10.1186/1472-6939-11-21

Wright, G.E.B., Koornhof, P.G.J., Adeyemo, A.A. and Tiffin, N. (2013), "Ethical and legal implications of whole genome and whole exome sequencing in African populations", *BMC Medical Ethics*, Vol. 14, available at: https://doi.org/10.1186/1472-6939-14-21

Xiao, L., Lewis, P. and Gibb, A. (2008), "Developing a security protocol for a distributed decision support system in a healthcare environment", *Proceedings of the 30th International Conference on Software Engineering (ICSE'08), ACM, New York, NY*.

Yaghmaei, E., van de Poel, I., Christen, M., Gordijn, B., Kleine, N., Loi, M., Morgan, G. and Weber, K. (2017), "Cybersecurity and ethics, CANVAS white paper 1", available at: https://ssrn.com/abstract=3091909

Young, R., Willis, E., Cameron, G. and Geana, M. (2014), "Willing but unwilling': attitudinal barriers to adoption of home-based health information technology among older adults", *Health Informatics Journal*, Vol. 20 No. 2, pp. 127-135, available at: https://doi.org/10.1177/1460458213486906

About the authors

Michele Loi is post-doctoral researcher at the Digital Society Initiative, University of Zurich, where he researches the ethics of digital technology, particularly big data and algorithms. Michele Loi is the corresponding author and can be contacted at: michele.loi@uzh.ch

Markus Christen is the Managing Director of the "Digital Society Initiative" of the University of Zurich (UZH) and heads the "Neuro-Ethics-Technology" research group at the Institute for Biomedical Ethics and Medical History at the UZH. His research areas are ethics of information and communication systems, neuroethics and empirical ethics.

Nadine Kleine is a Research Assistant in the EU project CANVAS and a PhD candidate in the graduate program "Trust and Acceptance in Extended and Virtual Work Environments" at the University of Osnabrueck. Her research interests include technology assessment, perception and acceptance, particularly in the domains of labor and health.

Karsten Weber is the Co-Head of the Institute for Social Research and Technology Assessment and one of the three Directors of the Regensburg Center of Health Sciences and Technology at the Technical University of Applied Sciences Regensburg. His research focuses on social and ethical impacts of information and communication technology, particularly with regard to health care and mobility.